CERIAS

The Center for Education and Research in Information Assurance and Security

Noise Detection of the Physical Data layer in EVs

Manuel Mar, Eric Dietz, Alissa Gilbert

1. Abstract: Vehicle Cybersecurity has become an important discipline, the prevention and study of possible attacks must be the most accurate possible. This study propose differentiate and analyze the relevant and useful data when trying to protect the Vehicle from cyber-threats.

2. Objectives

- Determine how much change there must be to affect the car performance
- Discriminate the useful data

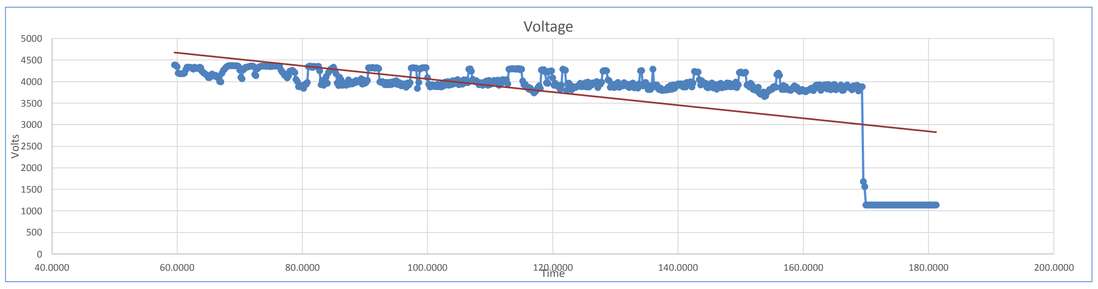
3. Problem: It is important to detect any undesirable changes in the car parameters in order to have a good car performance, however, drivers usually do not notice little changes in the cars that can damage the vehicle safety or even the driver itself. Thus by using the collected data of one EV go kart, this research will focus in looking for how much noise can be generated in the data without the driver noticing and try too look if this data is relevant at all.

4. Methodology: The data was collected from a electric go kart on the Purdue Grand Prix, Using the CAN bus system of the BMS and the VCS of the Curtis controller . Although all of this data was collected, that does not necessarily means it is useful to detect threat attacks.

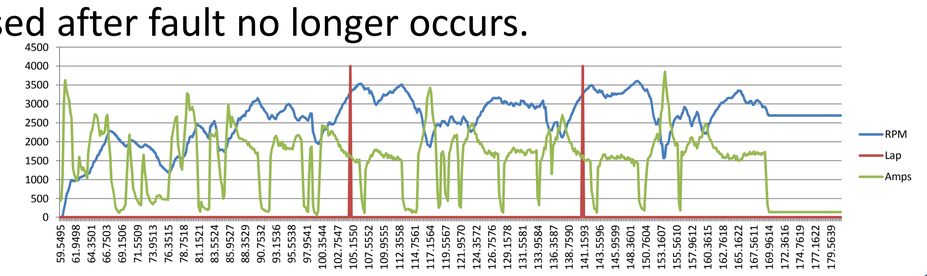
Value	Relevance
Mph	Medium
Voltage	High
Motor Temperature	Low
Controller Temperature	Low
RPM	Medium
Current	High

4.Results: We want to see the data simplified and look for changes that can affect the performance of the vehicle. For example the voltage of the motor, it can be seen the value remains constant until the car is turned off. Now the driver would not notice the little voltage changes in the chart and that is because it does not affect the performance at all, however, a sudden change could affect drastically the motor power without noticing the driver and reduce the lifespan of the motor.

$$P_{in} = 3\,V_{ph} I_{ph} cos\theta$$



This parameter may be relevant because affects directly to the car power (see equation), other parameter like the temperature of the battery and the motor, are less important, because this changes always occurs in a car and a any mechanical issue could cause that change not necessarily the a cyberattack. Usually this this data is erased after fault no longer occurs.



5.Findings/Analysis:

Faults are usually classified as either hard or soft. Soft faults are intermittent issues, whereas hard faults are ones that won't go away without some sort of intervention.

It is necessary to look for faults that do not trigger the malfunction indicator lamp. The MIL turn on with engine load, rpm, engine temperature and that something user can notice easily. So what are the other parameters are relevant, an attacker will freeze frame data to hide malicious activity, MIL then will not work if the voltage is constantly changing at the end the engine will suffer damage without noticing.

How much change must be present to detect vehicle cyber performance attacks?

	Range		Median	Error		SD
Voltage	3650	4400	3971	11%	8%	185.53
Amp	150	3800	1699	124%	96%	752.70
Power	10	283	125	127%	100%	54.34

6. Conclusion/Future Work:

The most important information in the data collected are not eh one that are common when a car runs, an attacker knows that. Consequently when trying to look for threats it result more important to focus on the parameter that are not obvious for drivers but important for drivers such as voltage and current in the CAN bus or the Diagnostic trouble codes storage.

In the future it is desirable to do an algorithm that discriminate useful data from the faults that can affect seriously the car physically and data that can affect the network of the car

PURDUE UNIVERSITY Discovery Park

CERIAS